REMARKS

The Applicants have respectfully amended independent Claims 1, 8 and 15 pursuant to the Examiner Interview on July 25, 2006 in order to clarify the functionality of the EMI code so as to further distinguished independent Claims 1, 8 and 15 over the cited references.

35 U.S.C. §103(a)

Claims 1-3, 6-10 and 14-20 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Pat. No. 6,028,932 ("Park"), in view of U.S. Pat. No. 6,058,476 ("Matsuzaki"). The Applicants respectfully disagree because the combination of Park and Matsuzaki do not disclose or suggest all elements in these claims, as amended.

Applicants respectfully direct the Examiner to amended independent Claim 1 that recites:

> wherein an unauthorized change in said EMI code from said first mode to said second mode, after said first encryption circuit encrypts said encoded information packet, causes decryption of said received information packet with said second decryption circuit, rendering said information packet inaccessible...

Accordingly, if the EMI code is changed without proper authorization, the received information packet is decrypted based on the newly changed EMI, rendering the information packet inaccessible because EMI indicates the proper encryption/decryption process. As such, changing the EMI after encrypting the information packet at the source causes the wrong encryption/decryption process to be used, rendering the information packet inaccessible.

In contrast, Park discloses a copy prevention apparatus where a key is inserted to a tape header of a bit stream, decrypted, and transmitted (see Park, col. 3, lines 58-63). Park further discloses that a key field is detected, which determines the copy prevention information, and the result is encrypted and outputted (see Park, col. 3 line 65 to col. 4 line 6). Park further discloses that the encryption key is transmitted and recorded (see Park, col. 2, lines 45-46). Accordingly, the bit stream is accessible if the transmission is intercepted. As such, a copy prevention information within a key field may be changed.

Amended independent Claim 1 distinguishes Park because it recites that an unauthorized change in the EMI code from the first mode to the second mode, after encrypting the information packet at the first encryption circuit, causes decryption of the received information packet with the second decryption circuit, rendering the information packet inaccessible.

Applicants respectfully assert that Matsuzaki, either alone or in combination with Park, fails to cure the deficiencies of Park discussed above with respect to independent Claims 1. Specifically, Matsuzaki also fails to teach or suggest the limitation that an "unauthorized change in said EMI code from said first mode to said second mode, after said first encryption circuit encrypts said encoded information packet, causes decryption of said received information

packet with said second decryption circuit, rendering said information packet inaccessible", as recited in independent Claim 1.

Accordingly, Park alone or in combination with Matsuzaki fails to teach the limitations of independent Claim 1. As such, independent Claim 1 is patentable over the combination of Park and Matsuzaki, under 35 U.S.C. 103(a). Amended independent Claims 8 and 15 recite limitations similar to that of independent Claim 1 and are patentable over the cited combination for similar reasons. Dependent claims are patentable by virtue of their dependency.

Additionally, dependent Claims 2, 9, and 17 further distinguish the combination of Park and Matsuzaki by reciting that the EMI code of the information packet is altered to the first mode by the sink device upon recording onto the recording medium. In contrast, Park discloses that a key is added to a reproduced bit stream, decrypted, and transmitted, and that the recording block searches for the key, extracts copy prevention information, encrypts, and records according to the extracted copy prevention information (see Park, col. 2, lines 60-67). As such, Park fails to disclose altering of the EMI code by the sink device, as claimed.

Moreover, dependent Claim 14 further distinguishes Park by reciting that the source and the sink device comprise of a first and a second hash circuit respectively. The Applicants have found no references in Park or Matsuzaki to a

hash circuit. In fact, Park only discloses that a key supply portion 107 encrypting messages and transmitting the result (see Park, col. 2, lines 19-20). Park neither discloses nor does it suggest that a hash circuit may be used. As such, Park does not disclose nor suggest the use of hash circuit as claimed.

As such, allowance of Claims 1-3, 6-10 and 14-20 is earnestly solicited.

Claims 1, 3-8, 10-13, 15-16 and 18 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Pat. No. 6,047,103 ("Yamauchi"), in view of Matsuzaki. The Applicants respectfully disagree because the combination of Yamauchi and Matsuzaki do not disclose or suggest all elements in these claims, as amended.

Yamauchi discloses that a user data is stored in the user data memory while CGMS control data is stored in CGMS control data memory wherein CGMS control data is used to manage the generation of copying by controlling reproduction of the sector (see Yamauchi, col. 26, lines 45-50). The encrypting circuit encrypts digital data to be output to the bus (see Yamauchi, col. 27, lines 15-16). When the authentication is successful, the microprocessor instructs the encrypting/authenticating unit to encrypt the digital data composed of the CGMS control data and to output the result to the controller (see Yamauchi, col. 30, lines 20-29). Accordingly, CGMS control data may be changed if the transmitted data is successfully intercepted and decrypted.

Amended independent Claim 1 distinguishes Yamauchi because it recites that an unauthorized change in the EMI code from the first mode to the second mode, after encrypting the information packet at the first encryption circuit, causes decryption of the received information packet with the second decryption circuit, rendering the information packet inaccessible.

Moreover, the rejection asserts that disk reproduction drive 126 in Yamauchi is a sink device. The rejection further asserts that an extractor circuit in the sink device for extracting EMI code is disclosed by a controller 128. Controller 128 is a separate component than the disk reproduction device 126 (See Yamauchi, Figure 15). As such, communication between the controller 128 and the reproduction drive exposes the data to potential unauthorized users and leaves it unprotected. As such, data may be intercepted and the CMGS control data and the user data may be changed, or reproduced.

Amended independent Claim 1 distinguishes Yamauchi because it recites that an extracting circuit is within the sink device. Therefore, data is protected and unexposed during a communication between the two units.

Furthermore, the rejection asserts that Yamauchi is considered to include a first encryption and a second encryption circuit, as claimed. The Applicants respectfully traverse because the cited portion of Yamauchi discloses only "an

encrypting section for converting the retrieved digital data into encrypted digital data" (see Yamauchi, col. 5, lines 60-61). Since Yamauchi discloses only one "encrypting section", the Applicants do not understand Yamauchi to either teach or suggest a first encryption circuit and a second encryption circuit, as claimed.

Applicants respectfully assert that Matsuzaki, either alone or in combination with Yamauchi, fails to cure the deficiencies of Yamauchi discussed above with respect to independent Claims 1. Specifically, Matsuzaki also fails to teach or suggest the limitation that an "unauthorized change in said EMI code from said first mode to said second mode, after said first encryption circuit encrypts said encoded information packet, causes decryption of said received information packet with said second decryption circuit, rendering said information packet inaccessible", as recited in independent Claim 1.

Accordingly, Yamauchi alone or in combination with Matsuzaki fails to teach the limitations of independent Claim 1. As such, independent Claim 1 is patentable over the combination of Yamauchi and Matsuzaki, under 35 U.S.C. 103(a). Independent Claims 8 and 15 recite limitations similar to that of independent Claim 1 and are patentable over the cited combination for similar reasons. Dependent claims are patentable by virtue of their dependency.

As such, allowance of Claims 1, 3-8, 10-13, 15-16 and 18 is earnestly solicited.

For the above reasons, the Applicants request reconsideration and withdrawal of these rejections under 35 U.S.C. §103.

CONCLUSION

In light of the above listed remarks, consideration of Claims 1-20 is requested. Based on the remarks presented above, it is respectfully submitted that Claims 1-20 are in condition for allowance.

Please charge any additional fees or apply any credits to our PTO deposit account number: 23-0085.

Respectfully submitted,
WAGNER, MURABITO & HAO LLP

Dated: Aug 7th, 2006

Amir A. Tabarrok
Registration No. 57,137

WAGNER, MURABITO & HAO LLP
Two North Market Street
Third Floor
San Jose, California 95113

(408) 938-9060 Voice
(408) 938-9069 Facsimile